EXHIBIT Q

UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF NEW YORK

State of New York, *et al.*	
Plaintiffs,	
v.	Case No. 1:25-cv-1144-JAV
U.S. Department of the Treasury, *et. al.*	
Defendants.	

I, Joseph Gioeli III, declare under penalty of perjury:

1. I currently serve as the Deputy Commissioner for Transformation and Modernization in the Bureau of the Fiscal Service (Bureau or BFS), in the U.S. Department of the Treasury (Treasury), and have been employed in this role since 2023. I report to the Commissioner of the Bureau. I am a career civil servant. Prior to my current position, I also served as the Bureau's Chief Technology Officer from 2017-2020 and its Chief Information Officer from 2020-2023. I have been employed at the Bureau for over seven years.

2. In my current role, I oversee, among other things, the Bureau's Office of Information and Security Services (ISS). ISS promotes the integrity and operational efficiency of the federal government's financial infrastructure that is within Treasury's responsibility, while ensuring the security of that infrastructure and the information it contains. In my position, I oversee the Chief Information Officer, who has authority over the security of and access to these systems. I have extensive knowledge of the Bureau's technology investments, as well as the related technology and cybersecurity strategies that support our enterprises.

3. I also understand the security posture of these systems, the types of data that generally transact through these systems, and their criticality to the national critical infrastructure. I am also familiar with Bureau requirements around access to sensitive systems.

4. In my current role, I have been involved in the Bureau's efforts to develop and implement a 4- to 6-week payment process engagement plan ("engagement") in which the Bureau would support Treasury employees from the Treasury DOGE Team in understanding payment processes and identifying opportunities to advance payment integrity and fraud reduction goals. The Treasury DOGE Team involved in this engagement consisted of Thomas Krause and Marko Elez. To date, to the best of my knowledge, Mr. Elez has been the only individual on the Treasury DOGE Team who has been provided direct access to BFS payment systems or source code. Mr. Krause had "over the shoulder" access by which he could view BFS payment systems or source code while they were being accessed by another person with the required access and permissions. I understand that Mr. Elez had provided Mr. Krause with updates about his work, which may have occasionally included screenshots of payment systems data or records, but Mr. Krause did not receive direct access to BFS payment systems or source code.

5. BFS has multiple payment and accounting systems that are responsible for different tasks and processes, which are involved in BFS's engagement with the DOGE team. These include Payment Automation Manager (PAM), Secure Payment System (SPS), Automated Standard Application for Payments (ASAP), International Treasury Services (ITS.gov), and the Central Accounting and Reporting System (CARS).

6. PAM is the primary application used by Treasury to process payments for disbursement, and it includes several components. PAM's "file system" is where payment files are transferred

2

from initiating agencies before processing and certification, sometimes referred to as its

"landing zone." Once certified by the initiating agency certifying official, PAM's "payment

processing system" processes the payments consistent with the instructions within the file.

The PAM payment process is described in more detail in the accompanying declaration of

Vona S. Robinson.

7. ASAP is a recipient-initiated electronic payment and information system; this means that it is

a payment system that allows recipients to draw down funds from an established account for

that recipient.

8. SPS is a system through which paying agencies securely create, certify, and submit

individual payment files to Treasury; it is also typically used for one-time large dollar amount

transactions.

9. International Treasury Services.gov (ITS) allows federal agencies to make international

payments, which are often used, for example, to provide Social Security benefit payments to

Americans living abroad.

10. Finally, the Central Accounting and Reporting System (CARS) is the electronic system for

recording the federal government's financial data on an agency's spending and provides

streamlined agency reporting for accounting purposes.

11. The scope of work as envisioned in the engagement plan required access to Fiscal Service

source code, applications, and databases across all these Fiscal Service payment and

accounting systems and their hosting environments. This broad access presented risks, which

included potential operational disruptions to Fiscal Service's payment systems, access to

sensitive data elements, insider threat risk, and other risks that are inherent to any user access

3

to sensitive IT systems. In light of these risks, BFS and Treasury Departmental Office employees developed mitigation strategies that sought to reduce these risks.

12. These measures included the requirement that Mr. Elez be provided with a BFS laptop, which would be his only method of connecting to the Treasury payments systems, both in connecting with the source code repository and for his read-only access of the systems. He had previously been provided a Treasury laptop from the Department shortly after he onboarded, but due to Bureau security policy, that device was restricted from accessing the BFS systems and services he had requested. BFS used several cybersecurity tools to monitor Mr. Elez's usage of his BFS laptop at all times and continuously log his activity. Additionally, the Bureau enabled enhanced monitoring on his laptop, which included the ability to monitor and block website access, block the use of external peripherals (such as USB drives or mass storage devices), monitor any scripts or commands executed on the device, and block access to cloud-based storage services. Additionally, the device contained data exfiltration detection, which alerts the Bureau to attempts to transmit sensitive data types. The laptop is also encrypted in accordance with Bureau policy, which, if the laptop were stolen or lost, would prevent unauthorized users from accessing data contained within the laptop.

13. Additional mitigation measures that were adopted included that Mr. Elez would receive "read-only" access to the systems, and that any reviews conducted using the "read-only" access would occur during low-utilization time periods, to minimize the possibility of operational disruptions. While providing a single individual with access to multiple systems and data records accessed here was broader in scope than what has occurred in the past, this read-only approach is similar to the kind of limited access the Bureau has provided to

4

auditors for other Treasury non-payment systems, though even in those scenarios the availability of production data was significantly limited.

14. Further, it was agreed that in the near-term only a single Treasury employee, Mr. Elez, would be designated as the "technical team member" who would exercise this read-only access. The Bureau would provide safeguarding and handling instructions for Treasury data for the duration of the project, and ISS personnel instructed Mr. Elez and Mr. Krause that no Treasury information and data could leave the Bureau laptop for the duration of the engagement, consistent with what was outlined in the engagement plan. The Treasury DOGE Team also agreed that, at the end of the project, it would provide the Bureau with an attestation statement that any copies of Treasury information made would be properly destroyed, and confirmation that no suspicious or unauthorized access to Bureau information or data had occurred during the engagement.

15. Overall, BFS and Treasury leadership were fully aware of the risks presented by Mr. Elez's work and sought to mitigate those risks to the extent possible through the measures just described.

16. On January 28, 2025, the Bureau provided Mr. Elez with the Bureau laptop and with copies of the source code for PAM, SPS, and ASAP in a separate, secure coding environment known as a "secure code repository" or "sandbox." Mr. Elez could review and make changes locally to copies of the source code in the cordoned-off code repository; however, he did not have the authority or capability to publish any code changes to the production system or underlying test environments. This repository was separate from Fiscal Service's typical code development environment, and unlike the usual code development environment, this

new repository was segmented, to ensure that no changes to the operative source code could be made.

17. On February 3, 2025, consistent with the engagement plan and mitigation measures developed, Mr. Elez was provided with read-only access, through his Bureau laptop, to the certain BFS systems. The read-only access that Mr. Elez was provided gives the user the ability to view and query information and data but does not allow for any changes to that information and data within its source system. While this reduces risk, it does not fully eliminate the risks identified in the assessment (for example, the risk of overburdening the system with a complex read-only query). Specifically, Mr. Elez was provided read-only access to the Payment Automation Manager (PAM) Database, Payment Automation Manager (PAM) File System, and, subsequently on February 5, the Secure Payment System (SPS) Database.

18. ISS configured his network access and assisted him in setting up the necessary tools to connect to the PAM database on February 3. His access was closely monitored by multiple BFS administrators throughout the process on February 3. That same day, he received a "walk-through" demonstration of two BFS payment systems, the PAM database and the PAM file system (the system that controls the payment file "landing zone" discussed above), to see how the systems worked. He logged in with his read-only access to these systems on February 3 during this "walk-through" demonstration. The Bureau is in the process of reviewing the logs of Mr. Elez's activity on his Bureau laptop, and this review remains ongoing. Based on the preliminary log reviews conducted to date, it appears that on February 3, Mr. Elez copied two USAID files directly from the PAM database to his BFS laptop; on February 4 and 5, Mr. Elez accessed the PAM file system; and on February 5, Mr. Elez

6

accessed the PAM payment processing database. These activities are consistent with the
read-only access that Mr. Elez was provided and did not change or alter any BFS payment
system or record within their source systems. As noted, reviews of Mr. Elez's work are still
actively occurring; I do not have any more detail to provide at this time about his activities
with respect to PAM.

19. Due to scheduling constraints, Mr. Elez was unable to meet with Bureau personnel to set up
his access to the SPS database until February 5. On that date, lSS held a virtual walk-through
session to help him to connect to the SPS database. He accessed this database exclusively
under the supervision of Bureau database administrators in a virtual walkthrough session.
According to the preliminary review of logs the Bureau has conducted to date, it appears Mr.
Elez accessed the SPS database only once during that walk-through demonstration on
February 5. It does not appear that he accessed the database again. As part of the ongoing
review, additional log reviews are currently underway to confirm this. Mr. Elez never logged
into ASAP, CARS, or ITS.gov, as technical access to those systems was never established for
him.

20. On the morning of February 6, it was discovered that Mr. Elez's database access to SPS on
February 5 had mistakenly been configured with read/write permissions instead of read-only.
A forensic investigation was immediately initiated by database administrators to review all
activities performed on that server and database. The initial investigation confirmed that all
of Mr. Elez's interactions with the SPS system occurred within the supervised, walk-through
session and that no unauthorized actions had taken place. His access was promptly corrected
to read-only, and he did not log into the system again after his initial virtual over-the-
shoulder session on February 5. To the best of our knowledge, Mr. Elez never knew of the

fact that he briefly had read/write permissions for the SPS database, and never took any action to exercise the "write" privileges in order to modify anything within the SPS database—indeed, he never logged in during the time that he had read/write privileges, other than during the virtual walk-through – and forensic analysis is currently underway to confirm this.

21. As noted above, the Bureau used several cybersecurity tools to monitor Mr. Elez's usage and continuously log his activity. While forensic analysis is still ongoing, Bureau personnel have conducted preliminary reviews of logs of his activity both on his laptop and within the systems and at this time have found no indication of any unauthorized use, of any use outside the scope that was directed by Treasury leadership, or that Mr. Elez used his BFS laptop to share any BFS payment systems data outside the U.S. Government.

22. On February 6, 2025, Mr. Elez submitted his resignation as a Treasury employee. After the Bureau received written notification from the Department confirming his resignation, it revoked or removed all physical and logical access and recovered all Treasury equipment, including his Treasury Departmental Offices and Bureau laptops, Treasury Departmental Offices government cell phone, and Treasury building access cards.

23. I have consulted with other BFS officials familiar with our access policies, and to date we have not identified any BFS policies (in effect either currently or prior to January 20, 2025) that disallow Federal employees from accessing the BFS payment and accounting systems identified above on the basis that they hold non-career (or political) appointments or are Special Government Employees.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: _2/11/25_   Signed: _____
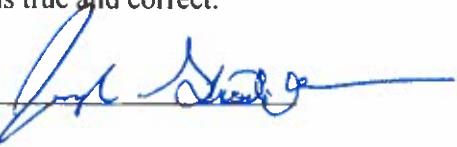
Joseph Gioeli III

Deputy Commissioner of Transformation and

Modernization

Bureau of the Fiscal Service

United States Department of the Treasury